

Univariate Niho Bent Functions from o-Polynomials

Lilya Budaghyan, Alexander Kholosha, Claude Carlet, and Tor Helleseeth, *Fellow, IEEE*

Abstract—In this paper, we discover that any univariate Niho bent function is a sum of functions having the form of Leander-Kholosha bent functions with extra coefficients of the power terms. This allows immediately, knowing the terms of an o-polynomial, to obtain the powers of the additive terms in the polynomial representing corresponding bent function. However, the coefficients are calculated ambiguously. The explicit form is given for the bent functions obtained from quadratic and cubic o-polynomials. We also calculate the algebraic degree of any bent function in the Leander-Kholosha class.

Index Terms—Bent function, Boolean function, maximum non-linearity, Niho bent function, o-polynomial, Walsh transform.

I. INTRODUCTION

Boolean functions of n variables are binary functions over the Galois field \mathbb{F}_{2^n} (or over the vector space \mathbb{F}_2^n of all binary vectors of length n). In this paper, we shall always endow this vector space with the structure of a field, thanks to the choice of a basis of \mathbb{F}_{2^n} over \mathbb{F}_2 . Boolean functions are used in the pseudo-random generators of stream ciphers and play a central role in their security.

Bent functions were introduced by Rothaus [1] in 1976. These are Boolean functions of even number of variables n , that are maximally nonlinear in the sense that their Hamming distance to all affine functions is optimal. This corresponds to the fact that their Walsh transform takes precisely the values $\pm 2^{n/2}$. Bent functions have also attracted a lot of research interest because of their relations to coding theory, sequences, and applications in cryptography. Despite their simple and natural definition, bent functions turned out to admit a very complicated structure in general. On the other hand, many special explicit constructions are known. Distinguished are primary constructions giving bent functions from scratch and secondary ones building new bent functions from one or several given bent functions.

Bent functions are often better viewed in their bivariate representation but can also be viewed in their univariate form (see Section II). A good survey reference containing information on explicit primary constructions of bent functions in their univariate form (expressed by means of the trace function) is [2], [3]. It is well known that some of these explicit constructions belong to the two general families of bent functions which are the original Maiorana-McFarland [4] and the Partial Spreads (\mathcal{PS}) classes. It was in the early 1970s when Dillon in his thesis [5] introduced the two above

mentioned classes and also another one denoted by H , where bentness is proven under some conditions which were not obvious to achieve (in this class, Dillon was able to exhibit only functions belonging, up to the affine equivalence, to the Maiorana-McFarland class).

It was observed in [6] that the class of the, so called, Niho bent functions (introduced in [7] by Dobbertin *et al*) is, up to EA-equivalence, equal to the Dillon's class H . Note that functions in class H are defined in their bivariate representation and Niho bent functions had originally a univariate form only. Three infinite families of Niho binomial bent functions were constructed in [7] and one of these constructions was later generalized by Leander and Kholosha [8] into a function with 2^r Niho exponents. Another class was also extended in [9]. In [10] it was proven that some of these infinite families of Niho bent functions are EA-inequivalent to any Maiorana-McFarland function which implies that classes H and Maiorana-McFarland are different up to EA-equivalence. New classes of Niho bent functions were also introduced in [6] thanks to the observed connection between class H and o-polynomials.

In this paper, we prove that any univariate Niho bent function is a sum of functions having the form of Leander-Kholosha bent function (see [8]) with extra coefficients of the power terms. In particular, any o-monomial corresponds to a 2^r term Niho bent function of Leander-Kholosha type with coefficients of the power terms inserted. This result allows immediately, knowing the terms of an o-polynomial, to obtain the powers of the additive terms in the polynomial representing corresponding bent function. However, the coefficients are calculated ambiguously. The explicit form is given for the bent functions obtained from quadratic and cubic o-polynomials. In general, we provide an explicit form for all Niho bent functions that correspond to o-monomials and o-polynomials of degree two and three. We also succeed in calculating the algebraic degree of any bent function in the Leander-Kholosha class. The paper is organized as follows. In Section II, we fix our main notation, recall the necessary background and, in Subsection II-C study the algebraic degree. Further, in Section III, we describe briefly the class \mathcal{H} introduced in [6] and give some necessary facts that we need later. The quadratic and cubic o-polynomials and their corresponding bent functions are considered in Sections V and VI.

II. NOTATION AND PRELIMINARIES

For any set E , denote $E \setminus \{0\}$ by E^* . Throughout the paper, let n be even and $n = 2m$.

L. Budaghyan, T. Helleseeth, and A. Kholosha are with the Department of Informatics, University of Bergen, P. O. Box 7803, N-5020 Bergen, Norway (e-mail: Lilya.Budaghyan@uib.no; Tor.Helleseeth@uib.no; Alexander.Kholosha@uib.no).

C. Carlet is with LAGA, UMR 7539, CNRS, Department of Mathematics, University of Paris 8 and University of Paris 13, 2 rue de la liberté, 93526 Saint-Denis Cedex, France (e-mail: claude.carlet@univ-paris8.fr).

A. Trace Representation, Boolean Functions in Univariate and Bivariate Forms

For any positive integer k and any r dividing k , the trace function $\text{Tr}_r^k(\cdot)$ is the mapping from \mathbb{F}_{2^k} to \mathbb{F}_{2^r} defined by

$$\text{Tr}_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}.$$

In particular, the *absolute trace* over \mathbb{F}_{2^k} is the function $\text{Tr}_1^k(x) = \sum_{i=0}^{k-1} x^{2^i}$ (in what follows, we just use $\text{Tr}_k(\cdot)$ to denote the absolute trace). Recall that the trace function satisfies the transitivity property $\text{Tr}_k = \text{Tr}_r \circ \text{Tr}_r^k$.

The univariate representation of a Boolean function is defined as follows: we identify \mathbb{F}_2^n (the n -dimensional vector space over \mathbb{F}_2) with \mathbb{F}_{2^n} and consider the arguments of f as elements in \mathbb{F}_{2^n} . An inner product in \mathbb{F}_{2^n} is $x \cdot y = \text{Tr}_n(xy)$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over \mathbb{F}_{2^n} that represents f (this is true for any vectorial function from \mathbb{F}_{2^n} to itself). The algebraic degree of f is equal to the maximum 2-weight of an exponent having nonzero coefficient, where the 2-weight $w_2(i)$ of an integer i is the number of ones in its binary expansion. Moreover, f being Boolean, its univariate representation can be written uniquely in the form of

$$f(x) = \sum_{j \in \Gamma_n} \text{Tr}_{o(j)}(a_j x^j) + a_{2^n-1} x^{2^n-1},$$

where Γ_n is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $2^n - 1$ (with respect to 2), $o(j)$ is the size of the cyclotomic coset containing j , $a_j \in \mathbb{F}_{2^{o(j)}}$ and $a_{2^n-1} \in \mathbb{F}_2$. The function f can also be written in a non-unique way as $\text{Tr}_n(P(x))$ where $P(x)$ is a polynomial over \mathbb{F}_{2^n} .

The bivariate representation of a Boolean function is defined as follows: we identify \mathbb{F}_2^n with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and consider the argument of f as an ordered pair (x, y) of elements in \mathbb{F}_{2^m} . There exists a unique bivariate polynomial $\sum_{0 \leq i, j \leq 2^m-1} a_{i,j} x^i y^j$ over \mathbb{F}_{2^m} that represents f . The algebraic degree of f is equal to $\max_{(i,j) | a_{i,j} \neq 0} (w_2(i) + w_2(j))$. And f being Boolean, its bivariate representation can be written in the form $f(x, y) = \text{Tr}_m(P(x, y))$, where $P(x, y)$ is some polynomial of two variables over \mathbb{F}_{2^m} .

B. Walsh Transform and Bent Functions

Let f be an n -variable Boolean function. Its “*sign*” function is the integer-valued function $\chi_f := (-1)^f$. The *Walsh transform* of f is the discrete Fourier transform of χ_f whose value at point $w \in \mathbb{F}_{2^n}$ is defined by

$$\hat{\chi}_f(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \text{Tr}_n(wx)}.$$

Definition 1: For even n , a Boolean function f in n variables is said to be *bent* if for any $w \in \mathbb{F}_{2^n}$ we have $\hat{\chi}_f(w) = \pm 2^{\frac{n}{2}}$.

It is well known (see, for instance, [2]) that the algebraic degree of a bent Boolean function in $n > 2$ variables is at most $\frac{n}{2}$. This means that in the univariate representation of a bent function, all exponents i whose 2-weight is larger than m

have zero coefficients a_i . If f is a bent function in n variables then its dual \tilde{f} is the Boolean function defined by

$$\hat{\chi}_{\tilde{f}}(w) = 2^{\frac{n}{2}} \chi_f(w).$$

Obviously, \tilde{f} is also bent and its dual is f itself.

Definition 2: Functions $f, g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ are *extended-affine equivalent* (in brief, EA-equivalent) if there exist affine permutation L of \mathbb{F}_2^n and an affine function $l : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that $g(x) = (f \circ L)(x) + l(x)$. A class of functions is *complete* if it is a union of EA-equivalence classes. The *completed class* is the smallest possible complete class that contains the original one.

C. Niho Power Functions

A positive integer d (always understood modulo $2^n - 1$ with $n = 2m$) is a *Niho exponent* and $t \rightarrow t^d$ is a *Niho power function* if the restriction of t^d to \mathbb{F}_{2^m} is linear or, equivalently, $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. As we consider $\text{Tr}_n(at^d)$ with $a \in \mathbb{F}_{2^n}$, without loss of generality, we can assume that d is in the normalized form, i.e., with $j = 0$. Then we have a unique representation $d = (2^m - 1)s + 1$ with $1 < s < 2^m + 1$. If some s is written as a fraction, this has to be interpreted modulo $2^m + 1$ (e.g., $1/2 = 2^{m-1} + 1$). Following are examples of bent functions consisting of one or more Niho exponents:

1. Quadratic function $\text{Tr}_m(at^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$ (here $s = 2^{m-1} + 1$).
2. Binomials of the form $f(t) = \text{Tr}_n(\alpha_1 t^{d_1} + \alpha_2 t^{d_2})$, where $2d_1 \equiv 2^m + 1 \pmod{2^n - 1}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^*$ are such that $(\alpha_1 + \alpha_1^{2^m})^2 = \alpha_2^{2^m+1}$. Equivalently, denoting $a = (\alpha_1 + \alpha_1^{2^m})^2$ and $b = \alpha_2$ we have $a = b^{2^m+1} \in \mathbb{F}_{2^m}^*$ and

$$f(t) = \text{Tr}_m(at^{2^m+1}) + \text{Tr}_n(bt^{d_2}).$$

We note that if $b = 0$ and $a \neq 0$ then f is a bent function listed under number 1. The possible values of d_2 are [7], [9]:

$$d_2 = (2^m - 1)3 + 1,$$

$$6d_2 = (2^m - 1) + 6 \text{ (taking } m \text{ even).}$$

These functions have algebraic degree m and do not belong to the completed Maiorana-McFarland class [10].

3. [8], [11] Take $1 < r < m$ with $\gcd(r, m) = 1$ and define

$$f(t) = \text{Tr}_n \left(a^2 t^{2^m+1} + (a + a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{d_i} \right), \quad (1)$$

where $2^r d_i = (2^m - 1)i + 2^r$ and $a \in \mathbb{F}_{2^n}$ is such that $a + a^{2^m} \neq 0$. This function has algebraic degree $r + 1$ (see Proposition 1) and belongs to the completed Maiorana-McFarland class [12]. On the other hand, the dual of f is not a Niho bent function [12].

4. Bent functions in a bivariate representation obtained from the known o-polynomials.

Consider the listed above two binomial bent functions. If $\gcd(d_2, 2^n - 1) = d$ and $b = \beta^d$ for some $\beta \in \mathbb{F}_{2^n}$ then b can be “absorbed” in the power term t^{d_2} by a linear substitution

of variable t . In this case, up to EA-equivalence, $b = a = 1$. In particular, this applies to any b when $\gcd(d_2, 2^n - 1) = 1$ that holds in both cases except when $d_2 = (2^m - 1)3 + 1$ with $m \equiv 2 \pmod{4}$ where $d = 5$. In this exceptional case, we can get up to three different classes (since exponents 1, 2 and 4 belong to the same cyclotomic coset) but the exact situation has to be further investigated.

Also, it can be easily seen that in function (1), up to EA-equivalence, we can assume $a + a^{2^m} = 1$. Indeed, let $a + a^{2^m} = b \in \mathbb{F}_{2^m}$ and substitute t in (1) for $b^{-1}t$. This results in a function having the same form as $f(t)$ except for a/b taken instead of a . It remains to note that $a/b + (a/b)^{2^m} = 1$. Also note that the conjugated exponent d_i is equal to

$$2^m((2^m - 1)i2^{-r} + 1) = (2^m - 1)(2^{m-r}i + 1) + 1$$

and, therefore, bent function (1) can be equivalently written as

$$\text{Tr}_n \left(a^2 t^{2^m+1} + (a + a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{(2^m-1)(2^{m-r}i+1)+1} \right). \quad (2)$$

We will use this representation when extending this class in the following sections.

Proposition 1: Function $f(t)$ in (2) has algebraic degree $r + 1$.

Proof: For any $i \in \{1, \dots, 2^{r-1} - 1\}$ take exponent $(2^{m-r}i + 1)(2^m - 1) + 1$ and analyze its binary expansion.

First, for any odd $l = \sum_{i=0}^{m-1} l_i 2^i$ being its binary expansion, we obtain

$$\begin{aligned} l(2^m - 1) &= \sum_{i=1}^{m-1} l_i 2^{m+i} + l_0 2^m - \sum_{i=0}^{m-1} l_i 2^i \\ &= \sum_{i=1}^{m-1} l_i 2^{m+i} + (l_0 - 1)2^m + 1 + \sum_{i=0}^{m-1} (1 - l_i) 2^i \\ &= \sum_{i=1}^{m-1} l_i 2^{m+i} + 1 + \sum_{i=1}^{m-1} (1 - l_i) 2^i \end{aligned}$$

since $l_0 = 1$. Therefore, for $l = 2^{m-r}i + 1$ we obtain

$$\begin{aligned} \text{wt}(l(2^m - 1) + 1) &= \text{wt}(2^m - 2 - (l - 1) + 2) + \text{wt}(l) - 1 \\ &= \text{wt}(2^m - 2^{m-r}i) + \text{wt}(i) \\ &= \text{wt}(2^r - i) + \text{wt}(i) \\ &= r - \text{wt}(i - 1) + \text{wt}(i) \\ &= r - s + 1, \end{aligned}$$

where $i = 2^s j$ with $s \geq 0$ and j odd.

Thus, the maximal weight of exponents in $f(t)$ is $r + 1$. We complete the proof by showing that all the exponents in (2) are cyclotomic inequivalent. Assume, on the contrary, there exist $i, j \in \{1, \dots, 2^{r-1} - 1\}$ with $i \neq j$ and $t \in \{0, \dots, 2^m - 1\}$ such that

$$\begin{aligned} 2^{m-r}i(2^m - 1) + 2^m &\equiv 2^t(2^{m-r}j(2^m - 1) + 2^m) \text{ or} \\ 2^{m-r}(2^m - 1)(2^t j - i) + 2^m(2^t - 1) &\equiv 0 \pmod{2^{2m} - 1} \end{aligned}$$

that holds only if $2^m - 1$ divides $2^t - 1$ that gives $t = m$ (for $t = 0$, obviously, $i = j$). This results in the following equivalence

$$2^{m-r}(2^m j - i) + 2^m \equiv 0 \pmod{2^m + 1}$$

that has a unique solution $i = 2^r - j$ modulo $2^m + 1$. These solutions are not good since we have that $0 < i < 2^{r-1}$. \square

Note that bent function is obtained in (1) also when $r > m + 1$. However, both r and $r - m$ in this case result in bent functions that are the same, up to addition of a linear term. Indeed, assume $r = m + s$ with $1 < s < m$ and $\gcd(s, m) = 1$. Then, after multiplying d_i by 2^{2m} (that is one modulo $2^n - 1$) we obtain

$$d_i = (2^m - 1)2^{m-s}i + 1 \quad \text{for } i = 1, \dots, 2^{m+s-1} - 1.$$

Since i can be reduced modulo $2^m + 1$, the last $(2^m + 1)(2^{s-1} - 2)$ power terms in (1) cancel out and we are left with the terms corresponding to $i = 1, \dots, 2^{m+1} - 2^{s-1} + 1$. For the same reason, more terms cancel out that shrinks the range to $i = 2^m - 2^{s-1} + 1, \dots, 2^m + 1$. Further, taking $i = 2^m - 2^{s-1} + 1$ we get

$$d_i = -2^{2m-1} + 2^{m-1} + 1 \equiv 2^{m-1}(2^m + 1) \pmod{2^{2m} - 1}$$

and $\text{Tr}_m^r(t^{d_i}) = 0$ since $t^{d_i} \in \mathbb{F}_{2^m}$. Also, taking $i = 2^m + 1$ we get $d_i \equiv 1 \pmod{2^{2m} - 1}$ that gives a linear term.

The remaining $2^{s-1} - 1$ terms correspond to $i = 2^m - 2^{s-1} + 2, \dots, 2^m$. Taking $i = 2^m - 2^{s-1} + 2$ we obtain that

$$\begin{aligned} 2^{m-s}i &= (2^{m-s} - 1)(2^m + 1) + 2^{m-1} + 2^{m-s} + 1 \\ &\equiv 2^{m-1} + 2^{m-s} + 1 \pmod{2^m + 1}. \end{aligned}$$

Therefore,

$$d_i = (2^m - 1)(2^{m-1} + 2^{m-s}i + 1) + 1 \text{ for } i = 1, \dots, 2^{s-1} - 1.$$

Finally,

$$\begin{aligned} 2^m d_i &= (2^m - 1)(2^{2m-1} + 2^{2m-s}i + 2^m + 1) + 1 \\ &\equiv (2^m - 1)(2^{m-1} - 2^{m-s}i + 1) + 1 \\ &= (2^m - 1)(2^{m-s}(2^{s-1} - i) + 1) + 1 \pmod{2^n - 1} \end{aligned}$$

which indicates that d_i are 2^m th powers of the exponents in (2) taken with $r = s$. Also raising to the power of 2^m does not change the coefficient $a + a^{2^m}$.

Consider the remaining case when $r = m + 1$ and

$$d_i = (2^m - 1)2^{m-1}i + 1 \quad \text{for } i = 1, \dots, 2^m - 1.$$

Obviously, for $i < 2^m - 1$,

$$\begin{aligned} 2^m d_i &= (2^m - 1)(2^{2m-1}i + 1) + 1 \\ &\equiv (2^m - 1)(-2^{m-1}i + 2^{2m-1} - 2^{m-1}) + 1 \\ &= (2^m - 1)(2^{m-1}(2^m - 1 - i)) + 1 \pmod{2^n - 1} \\ &= d_{2^m-1-i}. \end{aligned}$$

Therefore, all power terms in (2) cancel out except for the quadratic one and the one corresponding to $i = 2^m - 1$ having

$$d_{2^m-1} = (2^m - 1)2^{2m-1} + 1 \equiv 2^m \pmod{2^n - 1}$$

and we get

$$f(t) = \text{Tr}_n(a^2 t^{2^m+1} + (a + a^{2^m})t)$$

that is, ignoring the linear term, a quadratic bent function listed under number 1.

III. CLASS \mathcal{H} OF BENT FUNCTIONS

In his thesis [5], Dillon introduced the class of bent functions denoted by H . The functions in this class are defined in their bivariate form as

$$f(x, y) = \text{Tr}_m(y + xF(yx^{2^m-2})), \quad (3)$$

where $x, y \in \mathbb{F}_{2^m}$ and F is a permutation of \mathbb{F}_{2^m} such that $F(x) + x$ does not vanish and for any $\beta \in \mathbb{F}_{2^m}^*$, the function $F(x) + \beta x$ is 2-to-1 (i.e., the pre-image of any element of \mathbb{F}_{2^m} is either a pair or the empty set). The condition that $F(x) + x$ does not vanish is required only for (3) to belong to \mathcal{PS} but is not necessary for bentness. Dillon was just able to exhibit bent functions in H that also belong to the completed Maiorana-McFarland class. As observed by Carlet and Mesnager [6, Proposition 1], this class can be slightly extended into a class \mathcal{H} defined as the set of (bent) functions g satisfying

$$g(x, y) = \begin{cases} \text{Tr}_m(xG(\frac{y}{x})), & \text{if } x \neq 0 \\ \text{Tr}_m(\mu y), & \text{if } x = 0 \end{cases}, \quad (4)$$

where $\mu \in \mathbb{F}_{2^m}$ and G is a mapping from \mathbb{F}_{2^m} to itself satisfying the following necessary and sufficient conditions:

$$F : z \rightarrow G(z) + \mu z \text{ is a permutation on } \mathbb{F}_{2^m} \quad (5)$$

$$z \rightarrow F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \quad (6)$$

As proved in [6], condition (6) implies condition (5) and, thus, is necessary and sufficient for g being bent. Adding the linear term $\text{Tr}_m((\mu+1)y)$ to (4) we obtain the original Dillon function (3). Therefore, functions in \mathcal{H} and in the Dillon class are the same up to the addition of a linear term. It is observed in [6] that Niho bent functions are just functions in \mathcal{H} in the univariate representation.

Any mapping F on \mathbb{F}_{2^m} that satisfies (6) is called an *o-polynomial*. The only linear o-monomial is a Frobenius map

$$F(z) = z^{2^i} \quad \text{with} \quad \gcd(i, m) = 1.$$

As proven in [13], following is the list of *all existing* quadratic o-monomials.

1. $F(z) = z^6$ with m odd.
2. $F(z) = z^{2^{2k}+2^k}$ with $m = 4k - 1$.
3. $F(z) = z^{2^{3k+1}+2^{2k+1}}$ with $m = 4k + 1$.
4. $F(z) = z^{2^{2k}+2}$ with $m = 2k - 1$.
5. $F(z) = z^{2^{m-1}+2^{m-2}}$ with m odd.

In [14], it was shown that the only cubic o-monomial is

$$F(z) = z^{3 \cdot 2^k + 4} \quad \text{with} \quad m = 2k - 1.$$

It is conjectured that no other o-monomial exists. Further, two o-trinomials are found

$$\begin{aligned} F(z) &= z^{2^k} + z^{2^k+2} + z^{3 \cdot 2^k+4} & \text{with } m &= 2k - 1 \\ F(z) &= z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}} & \text{with } m &\text{ odd.} \end{aligned}$$

The remaining two known, up to equivalence, o-polynomials are Subiaco and Adelaide listed in [6].

Using (4), every o-polynomial results in a bent function in class \mathcal{H} (and vice versa). In particular, functions (1) with $a + a^{2^m} = 1$ are obtained from Frobenius map $z^{2^{m-r}}$ [12], binomial Niho bent functions with $d_2 = (2^m - 1)3 + 1$

correspond to Subiaco hyperovals [9] and functions with $6d_2 = (2^m - 1) + 6$ correspond to Adelaide hyperovals. In the following Section V, we find bent functions that correspond to all the existing quadratic o-monomials. In Section VI the same problem is resolved for all cubic o-monomials.

IV. GENERAL FORM OF A NIHO BENT FUNCTION

By definition, all exponents of monomials contained in the univariate representation of a Niho bent function are of the Niho type, i.e., have the form of $d = (2^m - 1)s + 1$ with $1 < s < 2^m + 1$. From the results in this section, in particular, it follows that in a Niho bent function, s is odd. Moreover, we prove that any Niho bent function, up to EA-equivalence, is obtained as a sum of the following functions

$$\text{Tr}_n \left(A_{2^{r-1}} t^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} A_i t^{(2^m-1)(2^{m-r}i+1)+1} \right) \quad (7)$$

with $0 < r < m$ and $A_i \in \mathbb{F}_{2^n}^*$. Each function making up the sum is defined by a monomial found in the corresponding o-polynomial and has a particular set of nonzero coefficients A_i . Parameter $0 < m - r < m$ is equal to the position of the least significant one-digit in the binary expansion of the exponent in this monomial. The whole sum also has the form of (7) (taken with the largest r found among all the additive components) but some terms may cancel out due to addition of coefficients. Note that (7) consists of the same power terms as Leander-Kholosha bent function (2) but also has a particular coefficient for each term.

Lemma 1: Take an integer $d \in \{1, \dots, 2^m - 1\}$ and let $l \in \{0, \dots, m - 1\}$ be the position of the least significant one-digit in the binary expansion of d . Take any $\lambda \in \mathbb{F}_{2^m}^*$ and define bivariate function $g(x, y) = \text{Tr}_m(\lambda x^{2^m-d} y^d)$ over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then the univariate form of $g(x, y)$ obtained using identities $x = t + t^{2^m}$ and $y = at + a^{2^m} t^{2^m}$, where $t \in \mathbb{F}_{2^n}$ and a is a primitive element of \mathbb{F}_{2^n} , has the form of (7) with $m - r = l$, plus a linear term.

Proof: Denote $I_k = \{0, \dots, k - 1\}$ for $k > 0$ and assume $I_0 = \emptyset$. Define $D \subset I_m$ such that $d = \sum_{i \in D} 2^i$. Also define $T \subset I_m$ such that $2^m - d = \sum_{i \in T} 2^i$. It is easy to see that

$$T = (I_m \setminus (D \cup I_l)) \cup \{l\}.$$

Note that $D \cap T = \{l\}$ and $D \cup T = I_m \setminus I_l$.

Further,

$$\begin{aligned} & (t + t^{2^m})^{2^m-d} (at + a^{2^m} t^{2^m})^d \\ &= \prod_{i \in T} (t^{2^i} + t^{2^{m+i}}) \prod_{j \in D} (a^{2^j} t^{2^j} + a^{2^{m+j}} t^{2^{m+j}}) \\ &= \sum_{\substack{c_i \in \{0,1\} \\ i \in T}} t^{\sum_{i \in T} (c_i 2^i + \overline{c_i} 2^{m+i})} \\ &\quad \times \sum_{\substack{s_j \in \{0,1\} \\ j \in D}} a^{\sum_{j \in D} (s_j 2^j + \overline{s_j} 2^{m+j})} t^{\sum_{j \in D} (s_j 2^j + \overline{s_j} 2^{m+j})} \\ &= \sum_{\substack{c_i, s_j \in \{0,1\} \\ i \in T, j \in D}} a^{\sum_{j \in D} (s_j 2^j + \overline{s_j} 2^{m+j})} \\ &\quad \times t^{\sum_{i \in T} (c_i 2^i + \overline{c_i} 2^{m+i}) + \sum_{j \in D} (s_j 2^j + \overline{s_j} 2^{m+j})} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\substack{c_i, s_l \in \{0,1\} \\ i \in I_m \setminus I_l}} a^{\sum_{i \in D \setminus \{l\}} (c_i 2^i + \overline{c_i} 2^{m+i}) + s_l 2^l + \overline{s_l} 2^{m+l}} \\
&\times t^{\sum_{j \in I_m \setminus I_l} (c_j 2^j + \overline{c_j} 2^{m+j}) + s_l 2^l + \overline{s_l} 2^{m+l}} \\
&= \sum_{\substack{c_i, s \in \{0,1\} \\ i \in I_m \setminus I_l}} a^{\sum_{i \in D \setminus \{l\}} (c_i 2^i + \overline{c_i} 2^{m+i}) + s 2^l + \overline{s} 2^{m+l}} \\
&\times t^{2^l c + 2^{m+l} (2^{m-l} - c - 1) + s 2^l + \overline{s} 2^{m+l}}, \tag{8}
\end{aligned}$$

where integer $c = (c_{m-1}, \dots, c_l)$ in its binary expansion with the least significant bit c_l and the line over a bit value denotes its complement. Note that $0 \leq c < 2^{m-l}$.

Now we make several observations on additive terms in (8):

- (i) Assume $c = 2^{m-l} - 1$ and $s = 1$. Then the corresponding term is equal to $a^d t^{2^m}$ since

$$\sum_{i \in D \setminus \{l\}} 2^i + 2^l = d.$$

- (ii) Take any $c \in \{0, \dots, 2^{m-l} - 2\}$ and $s = 1$. Then the power of t in the corresponding term is equal to

$$\begin{aligned}
&2^l c + 2^{m+l} (2^{m-l} - c - 1) + 2^l \\
&= 2^l (c + 1) + 2^{m+l} (2^{m-l} - c - 2) + 2^{m+l}
\end{aligned}$$

that is equal to the power of t in the term corresponding to $c + 1$ and $s = 0$.

In particular, taking $c = 2^{m-l-1} - 1$ with $s = 1$ (or $c = 2^{m-l-1}$ with $s = 0$) we obtain the same power of t equal to

$$\begin{aligned}
&2^l (2^{m-l-1} - 1) + 2^{m+l} (2^{m-l} - 2^{m-l-1}) + 2^l \\
&= 2^{m-1} (2^m + 1).
\end{aligned}$$

This exponent is a self-conjugate. The coefficient of this term is equal to $a^{\tilde{d}} + a^{2^m \tilde{d}}$ with

$$\begin{aligned}
\tilde{d} &= \sum_{i \in D \setminus \{l\}} (c_i 2^i + \overline{c_i} 2^{m+i}) + 2^l = \sum_{i \in D} (c_i 2^i + \overline{c_i} 2^{m+i}) \\
&= \begin{cases} d, & \text{if } m-1 \notin D \\ d + 2^{m-1} (2^m - 1), & \text{otherwise} \end{cases}
\end{aligned}$$

since $c = 2^{m-l-1} - 1$.

- (iii) Take any $c \in \{0, \dots, 2^{m-l} - 1\}$. The powers of t in the terms corresponding to c with $s = 1$ and $2^{m-l} - c - 1$ with $s = 0$ are conjugates since

$$\begin{aligned}
&(2^l c + 2^{m+l} (2^{m-l} - c - 1) + 2^l) 2^m \\
&\equiv 2^l (2^{m-l} - c - 1) + 2^{m+l} c + 2^{m+l} \pmod{2^n - 1}.
\end{aligned}$$

It is obvious that the powers of a in the terms corresponding to c with $s = 1$ and $2^{m-l} - c - 1$ with $s = 0$ are conjugates as well.

Therefore, we can fix $c_{m-1} = 1$, $s = 0$ and rewrite (8) as

$$\begin{aligned}
&\text{Tr}_m^n \left(a^d t^{2^m} + a^{\tilde{d}} t^{2^{m-1} (2^m + 1)} \right. \\
&+ \sum_{\substack{c_i \in \{0,1\}; c' > 0 \\ i \in I_{m-1} \setminus I_l}} \left(a^{\sum_{i \in D \setminus \{l\}} (c_i 2^i + \overline{c_i} 2^{m+i}) + 2^{m+l}} \right. \\
&+ a^{\sum_{i \in D \setminus \{l\}} (c_i^* 2^i + \overline{c_i^*} 2^{m+i}) + 2^l} \\
&\left. \left. \times t^{2^l c' + 2^{m+l} (2^{m-l-1} - c' - 1) + 2^{m-1} + 2^{m+l}} \right) \right) \\
&= \text{Tr}_m^n \left(a^d t^{2^m} + a^{\tilde{d}} t^{2^{m-1} (2^m + 1)} \right. \\
&+ \sum_{c'=1}^{2^{m-l-1}-1} A_{c'} t^{(2^m-1)2^l (2^{m-l-1}-c') + 2^m} \left. \right),
\end{aligned}$$

where $c' = (c_{m-2}, \dots, c_l)$ and $c' - 1 = (c_{m-2}^*, \dots, c_l^*)$ in its binary expansion with the least significant bit c_l and $A_i \in \mathbb{F}_{2^n}$ are defined explicitly. In particular, since a is a primitive element of \mathbb{F}_{2^n} , we conclude that all coefficients A_i are nonzero. In the case when $l = m - 1$ the sum over c_i is empty.

Finally, multiplying the latter expression by λ and placing it under the $\text{Tr}_m()$ function, ignoring the linear term $\text{Tr}_n(a^d t^{2^m})$, we obtain the expression having the form of (7) with $m - r = l$. \square

Observe some important properties of coefficients $A_{c'}$.

- (i) For any $c' \in \{1, \dots, 2^{m-l-2}\}$

$$A_{c'}^{2^m} = \begin{cases} A_{2^{m-l-1}-c'}, & \text{if } m-1 \notin D \\ a^{2^{m-1}(2^m-1)} A_{2^{m-l-1}-c'}, & \text{otherwise.} \end{cases}$$

Indeed, if $m-1 \notin D$ then

$$\begin{aligned}
A_{c'}^{2^m} &= a^{\sum_{i \in D \setminus \{l\}} (\overline{c_i^*} 2^i + c_i^* 2^{m+i}) + 2^{m+l}} \\
&+ a^{\sum_{i \in D \setminus \{l\}} (\overline{c_i} 2^i + c_i 2^{m+i}) + 2^l} = A_{2^{m-l-1}-c'}
\end{aligned}$$

since

$$(\overline{c_{m-2}^*}, \dots, \overline{c_l^*}) = 2^{m-l-1} - 1 - (c' - 1) = 2^{m-l-1} - c'$$

and

$$2^{m-l-1} - c' - 1 = (2^{m-l-1} - 1) - c' = (\overline{c_{m-2}}, \dots, \overline{c_l}).$$

Otherwise, if $m-1 \in D$ then

$$\begin{aligned}
A_{c'}^{2^m} &= a^{2^{2m-1} + \sum_{i \in D \setminus \{l, m-1\}} (\overline{c_i^*} 2^i + c_i^* 2^{m+i}) + 2^{m+l}} \\
&+ a^{2^{2m-1} + \sum_{i \in D \setminus \{l, m-1\}} (\overline{c_i} 2^i + c_i 2^{m+i}) + 2^l} \\
&= a^{2^{m-1} (2^m - 1)} A_{2^{m-l-1}-c'}.
\end{aligned}$$

- (ii) As a direct consequence we obtain that $A_{2^{m-l-2}} \in \mathbb{F}_{2^m}$ when $m-1 \notin D$ and $a^{-2^{m-1}} A_{2^{m-l-2}} \in \mathbb{F}_{2^m}$ when $m-1 \in D$.

- (iii) If c' is odd then

$$A_{c'} = a^{\sum_{i \in D \setminus \{l\}} (c_i 2^i + \overline{c_i} 2^{m+i})} (a^{2^m} + a)^{2^l}.$$

Theorem 1: Any Niho bent function in the univariate form, up to EA-equivalence, is obtained as a sum of functions having

the form of (7). Each function making up the sum is defined by a monomial found in the corresponding o-polynomial and has a particular set of nonzero coefficients A_i for $i = 1, \dots, 2^{r-1}$. Parameter $0 < m - r < m$ is equal to the position of the least significant one-digit in the binary expansion of the exponent in this monomial.

Proof: By (4), any Niho bent function in the bivariate form is equal to $g(x, y) = \text{Tr}_m(xF(yx^{2^m-2}) + \mu y)$, where $F(z)$ defines an o-polynomial over \mathbb{F}_{2^m} . The linear term $\text{Tr}_m(\mu y)$ can be dropped.

Polynomial $F(z)$ consists of power terms that can be treated separately under the trace using Lemma 1 and the results are added together. Note that the identities $x = t + t^{2^m}$ and $y = at + a^{2^m}t^{2^m}$ used in Lemma 1 to obtain univariate formulas for functions in a bivariate representation, assume a particular choice of a basis of \mathbb{F}_{2^n} as a two-dimensional vector space over \mathbb{F}_{2^m} . But we know that taking a different basis just results in EA-equivalent functions.

Finally, by [15, Result 1], all terms in an o-polynomial have even powers if $m > 1$, i.e., $m - r = l$ from Lemma 1 is not zero and $r < m$. \square

From the result proven it follows that, up to EA-equivalence, the leading term in a univariate polynomial giving a Niho bent function has degree cyclotomic equivalent to $2^m + 1$. This confirms the conjecture made in [7, Section 3] for the particular case of bent binomials. It also confirms that the only existing monomial Niho bent function is the quadratic one $\text{Tr}_m(at^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$. (need to check that the coefficient is nonzero???)

Note that the function $g(x, y) = \text{Tr}_m(\lambda x^{2^m-d} y^d)$ has algebraic degree $m + wt(d) - wt(d-1) = m - l + 1 \leq m$ since $m - r = l > 0$. Therefore, algebraic degree of a Niho bent function is at most m (as for any bent function).

V. NEW NIHO BENT FUNCTIONS FROM QUADRATIC O-MONOMIALS

In this section, we extend class (1) of bent functions for some particular values of m and r . This is done by inserting coefficients of the power terms. These coefficients take just one of four possible values and are repeated in the cycle of length 2^{c+1} . Here we calculate the corresponding function F and later, selecting particular parameters, we show that F is an o-polynomial. This gives the proof of bentness.

For any integer $m > 2$ take $n = 2m$ and select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take any $0 \leq J < I < m - 1$ and define

$$\begin{aligned} A_1 &= a^{2^I} + 1 \\ A_2 &= a^{2^I} + a^{2^J} \\ A_3 &= a^{2^I} + a^{2^J} + 1. \end{aligned}$$

Also fix integers $2 < r \leq m$ and $0 < c < r - 1$ used to define the following Boolean function over \mathbb{F}_{2^n}

$$\begin{aligned} f(t) &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) \\ &+ \text{Tr}_n \left(\sum_{j=0}^{2^{r-c-2}-1} \left(A_1 \sum_{i=1}^{2^c-1} t^{(2^{m-r}(2^{c+1}j+i)+1)(2^m-1)+1} \right. \right. \\ &\left. \left. + A_2 t^{(2^{m-r}(2^{c+1}j+2^c)+1)(2^m-1)+1} \right) \right) \end{aligned} \quad (9)$$

$$\begin{aligned} &+ A_1^{2^m} \sum_{i=2^c+1}^{2^{c+1}-1} t^{(2^{m-r}(2^{c+1}j+i)+1)(2^m-1)+1} \\ &+ \sum_{j=0}^{2^{r-c-2}-2} A_3 t^{(2^{m-r}(2^{c+1}j+2^c)+1)(2^m-1)+1} \end{aligned}.$$

In the case when $r - c = 2$ assume the last sum equal to zero.

It is easy to see that function (9) has the form of (7) with coefficients repeated in a cycle of length 2^{c+1} as follows

$$\begin{aligned} \underbrace{i}_{A_i} &= \underbrace{1, \dots, 2^c - 1}_{A_1}, \underbrace{2^c}_{A_2}, \underbrace{2^c + 1, \dots, 2^{c+1} - 1}_{A_1^{2^m}}, \underbrace{2^{c+1}}_{A_3}, \\ &\dots, 2^{r-1}. \end{aligned}$$

Note that w.l.o.g. we can assume

$$A_1 = a^{2^{I-J}} + 1, \quad A_2 = a^{2^{I-J}} + a, \quad A_3 = a^{2^{I-J}} + a + 1$$

since raising to the power 2^I ($I > 0$) permutes the set $\{a \in \mathbb{F}_{2^n} \mid a + a^{2^m} = 1\}$.

Further, note that $A_2, A_3 \in \mathbb{F}_{2^m}$ and $a + a^{2^m} = 1$ implies that $A_1^{2^m} + A_3 = A_1 + A_2$. Rewrite function $f(t)$ as

$$\begin{aligned} f(t) &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) \\ &+ \text{Tr}_n \left(\sum_{j=0}^{2^{r-c-2}-1} t^{2^{m-r+c+1}j(2^m-1)+2^m} \right. \\ &\times \left(A_1 \sum_{i=1}^{2^c} t^{2^{m-r}i(2^m-1)} + A_1^{2^m} \sum_{i=2^c+1}^{2^{c+1}} t^{2^{m-r}i(2^m-1)} \right. \\ &\left. \left. + (A_1 + A_2)(t^{2^{m-r+c}(2^m-1)} + t^{2^{m-r+c+1}(2^m-1)}) \right) \right) \\ &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) + \text{Tr}_n \left(\frac{t^{2^{m-1}(2^m-1)} + 1}{t^{2^{m-r+c+1}(2^m-1)} + 1} t^{2^m} \right. \\ &\times \left(A_1 \frac{(t^{2^{m-r+c}(2^m-1)} + 1)t^{2^{m-r}(2^m-1)}}{t^{2^{m-r}(2^m-1)} + 1} \right. \\ &+ A_1^{2^m} \frac{(t^{2^{m-r+c}(2^m-1)} + 1)t^{2^{m-r}(2^c+1)(2^m-1)}}{t^{2^{m-r}(2^m-1)} + 1} \\ &\left. \left. + (A_1 + A_2)(t^{2^{m-r+c}(2^m-1)} + t^{2^{m-r+c+1}(2^m-1)}) \right) \right) \\ &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) + \text{Tr}_n \left(\frac{t^{2^{m-1}(2^m+1)} + t^{2^m}}{(t^{2^m} + t)^{2^{m-r+c+1}}} \right. \\ &\times \left((t^{2^m+1} + t^2)^{2^{m-r+c}} t^{2^{2m-r}} \frac{A_1 + A_1^{2^m} t^{2^{m-r+c}(2^m-1)}}{(t^{2^m} + t)^{2^{m-r}}} \right. \\ &\left. \left. + (A_1 + A_2)(t^{2^m+1} + t^{2^{m+1}})^{2^{m-r+c}} \right) \right). \end{aligned}$$

Here, in the case when $t^{2^{m-1}} = 1$ we assume fractions are equal to zero.

Since $a \notin \mathbb{F}_{2^m}$, the pair $(a, 1)$ makes up a basis of \mathbb{F}_{2^n} as a two-dimensional vector space over \mathbb{F}_{2^m} . Then every element $t \in \mathbb{F}_{2^n}$ can be uniquely represented as $ax + y$ with $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Now if $x = 0$ then $t = y$ and we obtain

$$f(y) = \text{Tr}_m(A_3 y).$$

For $x \neq 0$, denoting $s = a + y/x$ and since $s^{2^m} + s = 1$, we obtain

$$\begin{aligned}
f(ax + y) &= \text{Tr}_m(A_3 s^{2^{m-1}(2^m+1)} x) \\
&+ \text{Tr}_n \left(x \frac{s^{2^{m-1}(2^m+1)} + s^{2^m}}{(s^{2^m} + s)^{2^{m-r+c}+1}} \right. \\
&\times \left((s^{2^m+1} + s^2)^{2^{m-r+c}} s^{2^{2m-r}} \frac{A_1 + A_1^{2^m} s^{2^{m-r+c}(2^m-1)}}{(s^{2^m} + s)^{2^{m-r}}} \right. \\
&\left. \left. + (A_1 + A_2)(s^{2^m+1} + s^{2^{m+1}})^{2^{m-r+c}} \right) \right) \\
&= \text{Tr}_m(A_3 s^{2^{m-1}(2^m+1)} x) + \text{Tr}_n \left(x(s^{2^{m-1}(2^m+1)} + s^{2^m}) \right. \\
&\times (s^{2^{2m-r}+2^{m-r+c}} (A_1 + A_1^{2^m} s^{2^{m-r+c}(2^m-1)}) \\
&\left. + (A_1 + A_2)(s + 1)^{2^{m-r+c}}) \right) \\
&= \text{Tr}_m(A_3 s^{2^{m-1}(2^m+1)} x) \\
&+ \text{Tr}_n \left(x(s^{2^{m-1}(2^m+1)} + s^{2^m}) ((s^{2^{m-r}} + 1) \right. \\
&\times (s^{2^{m-r+c}} + A_1^{2^m}) + (A_1 + A_2)(s^{2^{m-r+c}} + 1)) \left. \right) \\
&= \text{Tr}_m(A_3 s^{2^{m-1}(2^m+1)} x) \\
&+ \text{Tr}_n \left(x(s^{2^{m-1}(2^m+1)} + s^{2^m}) (s^{2^{m-r+c}+2^{m-r}} \right. \\
&+ (A_1 + A_2 + 1)s^{2^{m-r+c}} + A_1^{2^m} s^{2^{m-r}} + A_3) \left. \right) \\
&= \text{Tr}_m \left(x((s + 1)(a^{2^I} + a^{2^J} + 1) \right. \\
&+ s^{2^{m-r+c}+2^{m-r}} + a^{2^J} s^{2^{m-r+c}} + a^{2^I} s^{2^{m-r}}) \left. \right) \\
&= \text{Tr}_m \left(x(z^{2^{m-r+c}+2^{m-r}} + (a^{2^{m-r}} + a^{2^J}) z^{2^{m-r+c}} \right. \\
&+ (a^{2^{m-r+c}} + a^{2^I}) z^{2^{m-r}} + (a + z + 1)(a^{2^I} + a^{2^J} + 1) \\
&+ a^{2^I+2^{m-r}} + a^{2^J+2^{m-r+c}} + a^{2^{m-r+c}+2^{m-r}}) \left. \right) \\
&= \text{Tr}_m(xG(z)) ,
\end{aligned}$$

where $z = y/x$. Therefore, for any $x, y \in \mathbb{F}_{2^m}$,

$$f(ax + y) = \begin{cases} \text{Tr}_m(xG(y/x)), & \text{if } x \neq 0 \\ \text{Tr}_m(A_3 y), & \text{if } x = 0, \end{cases}$$

and

$$\begin{aligned}
F(z) &= G(z) + A_3 z \\
&= z^{2^{m-r+c}+2^{m-r}} + (a^{2^{m-r}} + a^{2^J}) z^{2^{m-r+c}} \\
&+ (a^{2^{m-r+c}} + a^{2^I}) z^{2^{m-r}} + (a + 1)(a^{2^I} + a^{2^J} + 1) \\
&+ a^{2^I+2^{m-r}} + a^{2^J+2^{m-r+c}} + a^{2^{m-r+c}+2^{m-r}} .
\end{aligned} \tag{10}$$

Note that

$$0 \leq m - r < m - 2 \quad \text{and} \quad m - r < m - r + c < m - 1 .$$

In particular, taking $J = m - r$ and $I = m - r + c$ we obtain

$$F(z) = z^{2^I+2^J} + \text{const} .$$

The full range is $0 \leq J < I < m$. So we have to consider separately the case when $I = m - 1$. If $J = m - 2$ then $F(z) = z^{2^{m-1}+2^{m-2}}$ and applying transformation $zF(z^{-1})$ we obtain $z^{2^{m-2}}$ that is a Frobenius o-polynomial if and only if m is odd. Transformation $zF(z^{-1})$ of o-polynomials translated in terms

of the associated bent functions results in a particular case of EA-equivalence (see 3.1.2 in [6]). Therefore, the quadratic o-polynomial listed under number 5 corresponds to the Niho bent function that is EA-equivalent to the function obtained from the Frobenius mapping $z^{2^{m-2}}$ with m odd.

For any integer $m > 1$ take $n = 2m$ and select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take any $0 \leq J < m - 1$ and define $r = m - J$,

$$A_1 = a^{2^{m-1}} \quad \text{and} \quad A_3 = a^{2^{m-1}} + a^{2^J}$$

for the following Boolean function over \mathbb{F}_{2^n}

$$\begin{aligned}
f(t) &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) \\
&+ \text{Tr}_n \left(A_1 \sum_{i=1}^{2^{r-1}-1} t^{(2^{m-r}i+1)(2^m-1)+1} \right) .
\end{aligned} \tag{11}$$

A. Bent Functions with 2^{m-2} Niho Exponents

Assume $m > 3$ is odd and take function (9) with $r = m - 1$, $c = 1$, $I = 2$ and $J = 1$. Then, by (10),

$$F(z) = z^6 + a^6 + (a + 1)(a^4 + a^2 + 1)$$

and, ignoring the constant term, this is an o-polynomial z^6 . Therefore, function (9) with such parameters is a bent function.

Note 1: This bent function can also have a more general form when taking any $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} \neq 0$. Define coefficients differently as

$$\begin{aligned}
A_1 &= a^{6 \cdot 2^m} + a^{2^{m+2}+2} \\
A_2 &= a^{2^{m+2}+2} + a^{2^{m+1}+4} \\
A_3 &= a^6 + a^{6 \cdot 2^m} .
\end{aligned}$$

Obviously, if $a + a^{2^m} = 1$ then these coefficients are the same as defined originally in this section. Still, this extension does not contain any new bent functions, up to EA-equivalence. Indeed, let $a + a^{2^m} = b \in \mathbb{F}_{2^m}$ and substitute t in the new function for $b^{-6}t$. This results in a similar function except for a/b taken instead of a . But $a/b + (a/b)^{2^m} = 1$ as we assumed originally.

Note 2: For $m = 3$, take any $a \in \mathbb{F}_{2^6}$ with $a + a^8 \neq 0$. Then for the basis $(a, 1)$, o-polynomial z^6 corresponds to the bent function that, up to the addition of a linear term, has the following form

$$f(t) = \text{Tr}_6(a^{36}t^{36}) + \text{Tr}_6(a^{22}t^{22}) .$$

Substituting at for t we obtain the EA-equivalent bent function $\text{Tr}_3(t^9) + \text{Tr}_6(t^{22})$ that is exactly function (1) with $r = m - 1 = 2$ and $a + a^{2^m} = 1$.

B. Bent Functions with 2^{m-k-1} Niho Exponents

Assume $m = 4k - 1 > 3$ and take function (9) with $r = 3k - 1$, $c = k$, $I = 2k$ and $J = k$. Then, by (10),

$$F(z) = z^{2^{2k}+2^k} + a^{2^{2k}+2^k} + (a + 1)(a^{2^{2k}} + a^{2^k} + 1)$$

and, ignoring the constant term, this is an o-polynomial $z^{2^{2k}+2^k}$. Therefore, function (9) with such parameters is a bent function.

Note 3: This bent function can also have a more general form when taking any $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} \neq 0$. Define coefficients differently as

$$\begin{aligned} A_1 &= a^{2^{m+2k}+2^{m+k}} + a^{2^{m+2k}+2^k} \\ A_2 &= a^{2^{m+2k}+2^k} + a^{2^{2k}+2^{m+k}} \\ A_3 &= a^{2^{m+2k}+2^{m+k}} + a^{2^{2k}+2^k} \end{aligned}$$

Obviously, if $a + a^{2^m} = 1$ then these coefficients are the same as defined originally in this section. Still, this extension does not contain any new bent functions, up to EA-equivalence. Indeed, let $a + a^{2^m} = b \in \mathbb{F}_{2^m}$ and substitute t in the new function for $b^{-(2^{2k}+2^k)}t$. This results in a similar function except for a/b taken instead of a . But $a/b + (a/b)^{2^m} = 1$ as we assumed originally.

Note 4: For $k = 1$, o-polynomial $z^{2^{2k}+2^k} = z^6$ is of Segre.

C. Bent Functions with 2^{m-2k-2} Niho Exponents

Assume $m = 4k + 1 > 5$ and take function (9) with $r = 2k$, $c = k$, $I = 3k + 1$ and $J = 2k + 1$. Then, by (10),

$$\begin{aligned} F(z) &= z^{2^{3k+1}+2^{2k+1}} + a^{2^{3k+1}+2^{2k+1}} \\ &\quad + (a + 1)(a^{2^{3k+1}} + a^{2^{2k+1}} + 1) \end{aligned}$$

and, ignoring the constant term, this is an o-polynomial $z^{2^{3k+1}+2^{2k+1}}$. Therefore, function (9) with such parameters is a bent function.

Note 5: This bent function can also have a more general form when taking any $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} \neq 0$. Define coefficients differently as

$$\begin{aligned} A_1 &= a^{2^{m+3k+1}+2^{m+2k+1}} + a^{2^{m+3k+1}+2^{2k+1}} \\ A_2 &= a^{2^{m+3k+1}+2^{2k+1}} + a^{2^{3k+1}+2^{m+2k+1}} \\ A_3 &= a^{2^{3k+1}+2^{2k+1}} + a^{2^{m+3k+1}+2^{m+2k+1}} \end{aligned}$$

Obviously, if $a + a^{2^m} = 1$ then these coefficients are the same as defined originally in this section. Still, this extension does not contain any new bent functions, up to EA-equivalence. Indeed, let $a + a^{2^m} = b \in \mathbb{F}_{2^m}$ and substitute t in the new function for $b^{-(2^{3k+1}+2^{2k+1})}t$. This results in a similar function except for a/b taken instead of a . But $a/b + (a/b)^{2^m} = 1$ as we assumed originally.

Note 6: For $k = 1$ (i.e., $m = 5$), o-polynomial z^{24} is obtained from the Frobenius mapping z^8 by transformation $zF(z^{-1})$ that preserves equivalence of o-polynomials and EA-equivalence of the corresponding bent functions (see 3.1.2 in [6]).

D. Bent Functions with 2^{m-2} Niho Exponents

Assume $m = 2k - 1 > 3$ and take function (9) with $r = m - 1$, $c = k - 1$, $I = k$ and $J = 1$. Then, by (10),

$$F(z) = z^{2^k+2} + a^{2^k+2} + (a + 1)(a^{2^k} + a^2 + 1)$$

and, ignoring the constant term, this is an o-polynomial z^{2^k+2} . Therefore, function (9) with such parameters is a bent function.

Note 7: Note that

$$(2^k + 2)(1 - 2^{k-1}) \equiv 1 \pmod{2^m - 1}$$

which means that the inverse of z^{2^k+2} is $z^{1-2^{k-1}}$. The latter is obtained from the Frobenius o-polynomial $z^{2^{k-1}}$ by transformation $zF(z^{-1})$ that preserves equivalence of o-polynomials (see 3.1.2 in [6]). Since the inverse of an o-polynomial is an o-polynomial we conclude that $z^{2^{k-1}}$ and z^{2^k+2} are equivalent o-polynomials.

Transformation $zF(z^{-1})$ of o-polynomials translated in terms of the associated bent functions results in a particular case of EA-equivalence. On the contrary, inverse o-polynomial does not correspond to the EA-equivalent bent function. This illustrates the case when two EA-inequivalent Niho bent functions arise from equivalent o-polynomials.

Note 8: For $k = 2$, o-polynomial $z^{2^k+2} = z^6$ is of Segre and for $k = 1$, $z^{2^k+2} = z^4$ is Frobenius mapping.

VI. NEW NIHO BENT FUNCTIONS FROM THE CUBIC O-MONOMIAL

In this section, we extend class (1) of bent functions for any odd m and $r = m - 2$. This is done by inserting coefficients of the power terms. These coefficients take just one of eight possible values and are repeated in the cycle of length $2^{(m+1)/2}$. Here we calculate the corresponding function F and showing that F is an o-polynomial, we give the proof of bentness.

For any integer m take $n = 2m$ and select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Take any $0 < J + 1 < I < m - 1$ and define

$$\begin{aligned} A_1 &= a^{3 \cdot 2^{I-1}} \\ A_2 &= a^{2^I} (a^{2^{I-1}} + a^{2^J}) \\ A_3 &= a^{3 \cdot 2^{I-1}+2^J} + (a + 1)^{3 \cdot 2^{I-1}+2^J} \end{aligned}$$

Also define the following Boolean function over \mathbb{F}_{2^n}

$$\begin{aligned} f(t) &= \text{Tr}_m(A_3 t^{2^{m-1}(2^m+1)}) \\ &\quad + \text{Tr}_n \left(\sum_{l=0}^{2^{m-I-2}-1} \left(A_1 \sum_{j=0}^3 a^{j2^{I-1}(2^m-1)} \sum_{i=1}^{2^{I-J-1}-1} t^{(2^J(2^{I-J-1}(4l+j)+i)+1)} \right. \right. \\ &\quad \left. \left. + A_2 \sum_{j=0}^2 a^{j2^{I-1}(2^m-1)} t^{(2^J(2^{I-J-1}(4l+j)+2^{I-J-1}+1)(2^m-1)+1)} \right. \right. \\ &\quad \left. \left. + A_3 \sum_{l=0}^{2^{m-I-2}-2} t^{(2^J(2^{I-J-1}(4l+3)+2^{I-J-1}+1)(2^m-1)+1)} \right) \right). \end{aligned} \quad (12)$$

In the case when $I = m - 2$ assume the last sum is equal to zero.

It is easy to see that function (12) has the form of (7) with coefficients repeated in a cycle of length 2^{c+1} (with $c = I - J$ and where $e = 2^{I-1}(2^m - 1)$) as follows

$$\begin{aligned} A_i &= \underbrace{1, \dots, 2^{c-1} - 1}_{A_1}, \underbrace{2^{c-1}}_{A_2}, \underbrace{2^{c-1} + 1, \dots, 2^c - 1}_{a^e A_1}, \underbrace{2^c}_{a^e A_2}, \\ &\quad \underbrace{2^c + 1, \dots, 3 \cdot 2^{c-1} - 1}_{a^{2e} A_1 = (a^e A_1)^{2^m}}, \underbrace{3 \cdot 2^{c-1}}_{a^{2e} A_2 = A_2^{2^m}}, \\ &\quad \underbrace{3 \cdot 2^{c-1} + 1, \dots, 2^{c+1} - 1}_{a^{3e} A_1 = A_1^{2^m}}, \underbrace{2^{c+1}}_{A_3}, \dots, 2^{m-J-1} \end{aligned}$$

Note that $a^e A_2 \in \mathbb{F}_{2^m}$.

TABLE I
NIHO BENT FUNCTIONS FROM EQUIVALENT O-MONOMIALS

m	$G_1(z)$	d_1	$G_2(z)$	d_2	$G_3(z)$	d_3
$2k-1$	2^k	k	2^{k-1}	$k+1$	2^k+2	m
$4k+1$	6	m	$\sum_{i=0}^{\frac{m-3}{2}} 2^{2i+1} + 2^{m-1}$	m	$2 + \sum_{i=1}^k 2^{4i} + \sum_{i=1}^k 2^{4i-1}$	m
$4k+3$					$4 + \sum_{i=1}^k 2^{4i} + \sum_{i=1}^k 2^{4i+1}$	$m-1$
$4k-1$	$2^{2k} + 2^k$	$3k$	$2^m - 2^{3k-1} + 2^{2k} - 2^k$	$3k$	$2 + \sum_{i=1}^{\frac{k-1}{2}} 2^{2i} + \sum_{i=\frac{k-3}{2}}^{\frac{3k-3}{2}} 2^{2i+1}$ $2^k + \sum_{i=\frac{k}{2}}^{\frac{3k-2}{2}} 2^{2i+1} + \sum_{i=\frac{3k}{2}}^{2k-1} 2^{2i}$	m^* $3k^\dagger$
$4k+1$	$2^{3k+1} + 2^{2k+1}$	$2k+1$	$2^m - 2^{3k+1} + 2^{2k+1} - 2^k$	$3k+2$	$2^{k+1} + \sum_{i=\frac{k+1}{2}}^{\frac{3k-1}{2}} 2^{2i+1} + \sum_{i=\frac{3k+1}{2}}^{2k} 2^{2i}$ $2 + \sum_{i=1}^{\frac{k}{2}} 2^{2i} + \sum_{i=\frac{k}{2}}^{\frac{3k-2}{2}} 2^{2i+1}$	$3k+1^\ddagger$ m^\dagger
$2k-1$	$3 \cdot 2^k + 4$	$m-1$	$3 \cdot 2^{k-1} - 2$	m	$2^k + \sum_{i=\frac{k+1}{2}}^{k-1} 2^{2i}$ $2 + \sum_{i=1}^{\frac{k-2}{2}} 2^{2i}$	k^* m^\S

* $k > 1$ odd

$^\dagger k > 0$ even

$^\ddagger k$ odd

$^\S k > 2$ even

TABLE II
NIHO BENT FUNCTIONS FROM EQUIVALENT O-POLYNOMIALS

m	$G_1(z)$	d_1	$G_2(z)$	d_2	$G_3(z)$	d_3
$2k-1$	$z^{2^k} + z^{2^k+2} + z^{3 \cdot 2^k+4}$	m^*	$z(z^{2^k+1} + z^3 + z)^{2^{k-1}-1}$	m		
odd	$z^{\frac{1}{6}} + z^{\frac{1}{2}} + z^{\frac{5}{6}}$	m			$zG_2(z^{-1})$	

* $k > 2$

Further, note that

$$\begin{aligned}
& A_2 a^{3 \cdot 2^{I-1}(2^m-1)} + A_3 \\
&= (a+1)^{3 \cdot 2^{I-1}} + a^{2^{I-1}(3 \cdot 2^m-1)+2^J} + a^{3 \cdot 2^{I-1}+2^J} + (a+1)^{3 \cdot 2^{I-1}+2^J} \\
&= a^{2^J} (a+1)^{3 \cdot 2^{I-1}} + a^{2^{I-1}(3 \cdot 2^m-1)+2^J} + a^{3 \cdot 2^{I-1}+2^J} \\
&= a^{2^J} (a^{2^I} + a^{2^{I-1}} + 1) + a^{2^{I-1}(3 \cdot 2^m-1)+2^J} \\
&= a^{2^J-2^{I-1}} (a^{3 \cdot 2^{I-1}} + a^{2^I} + a^{2^{I-1}} + (a+1)^{3 \cdot 2^{I-1}}) \\
&= a^{2^J-2^{I-1}}
\end{aligned}$$

and rewrite function $f(t)$ as

$$\begin{aligned}
f(t) &= \text{Tr}_n \left(a^{3 \cdot 2^{I-1}+2^J} t^{2^{m-1}(2^m+1)} \right. \\
&\quad + \sum_{l=0}^{2^m-I-2-1} \left(A_1 \sum_{i=1}^{2^{I-J-1}} t^{2^J(2^{I-J+1}l+i)(2^m-1)+2^m} \sum_{j=0}^3 (at)^{j2^{I-1}(2^m-1)} \right. \\
&\quad + (A_1 + A_2) t^{2^{I-1}(4l+1)(2^m-1)+2^m} \sum_{j=0}^3 (at)^{j2^{I-1}(2^m-1)} \\
&\quad \left. \left. + (A_2 a^{3 \cdot 2^{I-1}(2^m-1)} + A_3) t^{2^{I+1}(l+1)(2^m-1)+2^m} \right) \right) \\
&= \text{Tr}_n \left(a^{3 \cdot 2^{I-1}+2^J} t^{2^{m-1}(2^m+1)} \right. \\
&\quad + t^{2^{m+J}} \frac{(t^{2^{m-1}(2^m+1)} + t^{2^m})(t^{2^m} + t)^{2^{I-1}} ((at)^{2^m} + at)^{2^{I+1}}}{(t^{2^m} + t)^{2^{I+1}+2^J} ((at)^{2^m} + at)^{2^{I-1}}} \\
&\quad + a^{2^J-2^{I-1}} t^{2^{m+I-1}} \frac{(t^{2^{m-1}(2^m+1)} + t^{2^m})((at)^{2^m} + at)^{2^{I+1}}}{(t^{2^m} + t)^{2^{I+1}} ((at)^{2^m} + at)^{2^{I-1}}} \\
&\quad \left. + a^{2^J-2^{I-1}} t^{2^{m+I+1}} \frac{t^{2^{m-1}(2^m+1)} + t^{2^m}}{(t^{2^m} + t)^{2^{I+1}}} \right) \\
&= \text{Tr}_n \left(a^{3 \cdot 2^{I-1}+2^J} t^{2^{m-1}(2^m+1)} \right. \\
&\quad \left. + t^{2^{m+J}} \frac{(t^{2^{m-1}(2^m+1)} + t^{2^m})((at)^{2^m} + at)^{3 \cdot 2^{I-1}+2^J}}{(at)^{2^m} + at} \right)
\end{aligned}$$

Here, in the case when $t^{2^m-1} = 1$ or $(at)^{2^m-1} = 1$ we assume the relevant fractions are equal to zero.

Since $a \notin \mathbb{F}_{2^m}$, the pair $(a+1, 1)$ makes up a basis of \mathbb{F}_{2^n} as a two-dimensional vector space over \mathbb{F}_{2^m} . Then every element $t \in \mathbb{F}_{2^n}$ can be uniquely represented as $(a+1)x + y$ with $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Now if $x = 0$ then $t = y$ and we obtain

$$f(y) = \text{Tr}_m(A_3 y) .$$

For $x \neq 0$, denoting $s = a + 1 + y/x$ and since $s^{2^m} + s = 1$, we obtain

$$\begin{aligned} f((a+1)x + y) &= \text{Tr}_n \left(a^{3 \cdot 2^{I-1} + 2^J} s^{2^{m-1}(2^m+1)} x \right. \\ &\quad + s^{2^{m+J}} x \frac{(s^{2^{m-1}(2^m+1)} + s^{2^m})((as)^{2^m} + as)^{3 \cdot 2^{I-1}}}{(s^{2^m} + s)^{3 \cdot 2^{I-1} + 2^J}} \\ &\quad + a^{2^J - 2^{I-1}} s^{2^{m+I-1}} x \frac{(s^{2^{m-1}(2^m+1)} + s^{2^m})((as)^{2^m} + as)^{3 \cdot 2^{I-1}}}{(s^{2^m} + s)^{2^{I+1}}} \\ &\quad \left. + a^{2^J - 2^{I-1}} s^{2^{m+I+1}} x \frac{s^{2^{m-1}(2^m+1)} + s^{2^m}}{(s^{2^m} + s)^{2^{I+1}}} \right) \\ &= \text{Tr}_n \left(a^{3 \cdot 2^{I-1} + 2^J} s^{2^{m-1}(2^m+1)} x \right. \\ &\quad + x(s^{2^{m+J}} + a^{2^J - 2^{I-1}} s^{2^{m+I-1}})(s^{2^{m-1}(2^m+1)} + s^{2^m})(a + s + 1)^{3 \cdot 2^{I-1}} \\ &\quad \left. + a^{2^J - 2^{I-1}} s^{2^{m+I+1}} x(s^{2^{m-1}(2^m+1)} + s^{2^m}) \right) \\ &= \text{Tr}_n \left(a^{3 \cdot 2^{I-1} + 2^J} s^{2^{m-1}(2^m+1)} x \right. \\ &\quad + x(z^{3 \cdot 2^{I-1} + 2^J} + a^{3 \cdot 2^{I-1} + 2^J})(s^{2^{m-1}(2^m+1)} + z + a) \Big) \\ &= \text{Tr}_m \left(x(z^{3 \cdot 2^{I-1} + 2^J} + a^{3 \cdot 2^{I-1} + 2^J})(z + a) \right. \\ &\quad + x(z^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J})(z + a + 1) \Big) \\ &= \text{Tr}_m \left(x(a^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J})(z + a) \right. \\ &\quad \left. + x(z^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J}) \right) \\ &= \text{Tr}_m(xG(z)) , \end{aligned}$$

where $z = y/x$. Therefore, for any $x, y \in \mathbb{F}_{2^m}$,

$$f((a+1)x + y) = \begin{cases} \text{Tr}_m(xG(y/x)), & \text{if } x \neq 0 \\ \text{Tr}_m(A_3 y), & \text{if } x = 0 , \end{cases}$$

and

$$\begin{aligned} F(z) &= G(z) + A_3 z \\ &= a(a^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J}) \\ &\quad + z^{3 \cdot 2^{I-1} + 2^J} + (a+1)^{3 \cdot 2^{I-1} + 2^J} \\ &= z^{3 \cdot 2^{I-1} + 2^J} + a^{3 \cdot 2^{I-1} + 2^J + 1} + (a+1)^{3 \cdot 2^{I-1} + 2^J + 1} . \end{aligned}$$

In particular, take $m = 2k - 1 > 5$ and $I = k + 1$, $J = 2$. Then

$$F(z) = z^{3 \cdot 2^k + 4} + a^{3 \cdot 2^k + 5} + (a+1)^{3 \cdot 2^k + 5}$$

and, ignoring the constant term, this is an o-polynomial $z^{3 \cdot 2^k + 4}$. Therefore, function (12) with such parameters is a bent function.

Note 9: For $k = 2$ (i.e., $m = 3$), o-polynomial $z^{3 \cdot 2^k + 4} = z^{16} = z^2$ is Frobenius mapping. For $k = 3$ (i.e., $m = 5$), o-polynomial $z^{3 \cdot 2^k + 4} = z^{28}$ is obtained from the Frobenius mapping z^4 by transformation $zF(z^{-1})$ that preserves equivalence of o-polynomials and EA-equivalence of the corresponding bent functions (see 3.1.2 in [6]).

Now it is easy to find a Niho bent function that corresponds to the following o-trinomial of degree three

$$F(z) = z^{2^k} + z^{2^k+2} + z^{3 \cdot 2^k+4} \quad \text{with } m = 2k - 1 .$$

Assume $n = 2m$ with $m = 2k - 1 > 5$ and select $a \in \mathbb{F}_{2^n}$ with $a + a^{2^m} = 1$. Since $F(z)$ is a sum of three o-monomials, we need to take a sum of three Niho bent functions that correspond to each of them. The first linear term is a Frobenius map that gives bent function (1) with $r = k - 1$. The second term is quadratic and corresponds to bent function (9) taken with $r = m - 1$, $c = k - 1$, $I = k$ and $J = 1$. Finally, the third term of degree three corresponds to the bent function (12) (because of a differently chosen basis in this case we need to take $a + 1$ in stead of a in coefficients A_1, A_2, A_3). Added together, the resulting bent function has the form of (1) with $r = m - 1$ and coefficients of power terms taking on one of at most ten different values.

VII. CONCLUSIONS

From our main results in Section V it follows that for any odd $m > 5$ there exist three (two for $m = 5$) classes of Niho bent functions that have the form of (9). These functions correspond to quadratic o-monomials. Up to EA-equivalence, these cases cover all the existing quadratic o-monomials.

In Table I, we present exponents for o-monomials $G_i(z)$, where $G_2(z) = G_1^{-1}(z)$ and $G_3(z) = (zG_2(z^{-1}))^{-1}$; d_i is the algebraic degree of a Niho bent function obtained from $G_i(z)$. Explicit expressions for $G_3(z)$ can be verified directly using formulas found in [16, Chap 5]. Since two EA-equivalent functions have the same algebraic degree, one can easily make conclusions on EA-inequivalence of many of the Niho bent functions arising from quadratic o-monomials using data in Table I. We also checked with a computer that for $m = 5$, the Niho bent function corresponding to z^{2^k+2} is EA-inequivalent to any of the Niho function of degree m contained in (2)-(3) of Subsection II-C and to any function arising from G_1, G_2 , and G_3 with $G_1(z) = z^6$. Further, for $m = 5$ and $G_1(z) = z^6$ we got that the Niho bent functions arising from G_1, G_2 , and G_3 are mutually EA-equivalent but they are EA-inequivalent to any Niho function of degree m contained in (2)-(3) of Subsection II-C.

REFERENCES

- [1] O. S. Rothaus, "On "bent" functions," *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, May 1976.
- [2] C. Carlet, "Boolean functions for cryptography and error-correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ser. Encyclopedia of Mathematics and its Applications, Y. Crama and P. L. Hammer, Eds. Cambridge: Cambridge University Press, 2010, vol. 134, ch. 8, pp. 257–397.
- [3] A. Kholosha and A. Pott, "Bent and related functions," in *Handbook of Finite Fields*, ser. Discrete Mathematics and its Applications, G. L. Mullen and D. Panario, Eds. London: CRC Press, 2013, ch. 9.3, pp. 255–265.

- [4] R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combin. Theory Ser. A*, vol. 15, no. 1, pp. 1–10, Jul. 1973.
- [5] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.
- [6] C. Carlet and S. Mesnager, "On Dillon's class H of bent functions, Niho bent functions and o-polynomials," *J. Combin. Theory Ser. A*, vol. 118, no. 8, pp. 2392–2410, Nov. 2011.
- [7] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions," *J. Combin. Theory Ser. A*, vol. 113, no. 5, pp. 779–798, Jul. 2006.
- [8] G. Leander and A. Kholosha, "Bent functions with 2^r Niho exponents," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5529–5532, Dec. 2006.
- [9] T. Helleseeth, A. Kholosha, and S. Mesnager, "Niho bent functions and Subiaco hyperovals," in *Theory and Applications of Finite Fields*, ser. Contemporary Mathematics, M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, Eds., vol. 579. Providence, Rhode Island: American Mathematical Society, 2012, pp. 91–101.
- [10] L. Budaghyan, C. Carlet, T. Helleseeth, A. Kholosha, and S. Mesnager, "Further results on niho bent functions," *IEEE Trans. Inf. Theory*, 2012, accepted.
- [11] N. Li, T. Helleseeth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4662–4667, Jul. 2013.
- [12] C. Carlet, T. Helleseeth, A. Kholosha, and S. Mesnager, "On the dual of bent functions with 2^r Niho exponents," in *Proceedings of the 2011 IEEE International Symposium on Information Theory*. IEEE, Jul./Aug. 2011, pp. 657–661.
- [13] W. E. Cherowitzo and L. Storme, " α -Flocks with oval herds and monomial hyperovals," *Finite Fields Appl.*, vol. 4, no. 2, pp. 185–199, Apr. 1998.
- [14] T. L. Vis, "Monomial hyperovals in Desarguesian planes," Ph.D. dissertation, University of Colorado Denver, 2010.
- [15] W. G. Chambers, "Clock-controlled shift registers in binary sequence generators," *IEE Proceedings - Computers and Digital Techniques*, vol. 135, no. 1, pp. 17–24, Jan. 1988.
- [16] D. G. Glynn, "Two new sequences of ovals in finite Desarguesian planes of even order," in *Combinatorial Mathematics X*, ser. Lecture Notes in Mathematics, L. R. A. Casse, Ed., vol. 1036. Berlin: Springer-Verlag, 1983, pp. 217–229.